In: Horizons in Computer Science Research. Volume 10 ISBN: 978-1-63463-740-4
Editor: Thomas S. Clary, pp. 1-33

Chapter 1

TELECOMMUNICATION NETWORK SECURITY

Muhammad Adeka*, Simon Shepherd† and Raed Abd-Alhameed‡
School of Engineering and Informatics, University of Bradford,
Bradford, West Yorkshire, UK

1. Introduction

After having been held for long in logical and physical isolation from other systems, telecommunication networks and other elements of critical infrastructure are rapidly being assimilated into the Internet, as illustrated in Figure 1. This practically defines the ubiquity of Internet as an indispensable ICT (Information and Communication Technology) infrastructural facility in this age of globalisation. Nowadays, with mere clicks using a mouse, systems including electrical grids and traffic systems are now accessible to users, regardless of their location and state of equilibrium; whether static or mobile. As a research has demonstrated,[1,2] such interconnectivity is not without consequences. With the bandwidth available to most cable modems, an adversary can launch attacks capable of denying voice service to cellular telecommunications networks in major cities. In times of emergency, when such networks are essential in saving lives, such attacks could be extremely dangerous.

A telecommunication system is indeed a communication system with the distinguishing keyword, the Greek *tele-*, which means "atadistance", to imply that the source and sink of the system are at some distance apart. Its purpose is to transfer information from some source to a distant user; the key concepts being *information*, *transmission* and *distance*.

With the involvement of distance, telecommunication requires some technique which incorporates a means, each, to send, convey and receive the information with some degree of fidelity that is acceptable to both the source and the sink. Figure 2 shows these basic components. The need for a fidelity criterion brings into focus the requirement for a limit on information capacity associated with a given system. The capacity may be defined in terms of a maximum information rate, in bits per second, or in terms of

* E-mail address: M.I.Adeka@student.Bradford.ac.uk
† E-mail address: S.J.Shepherd@Bradford.ac.uk
‡ E-mail address: R.A.A.Abd@Bradford.ac.uk

bandwidth. Intervening distance also brings attention to the need for a system that is attenuation effective, less cumbersome, relatively immune from interference and electromagnetic noise, *secure* and provides room for upgrading with as little economic and technical costs as possible. [3] This chapter is primarily concerned with the *security* aspect of telecommunication systems. In this chapter, unless otherwise specified, whenever the term c*ommunication(s)* is used, it equally denotes *telecommunication(s)* as explained earlier. Similarly, since the entire ICT world is mostly computerised, the focus will be on computer-mediated communications and cyber-space.

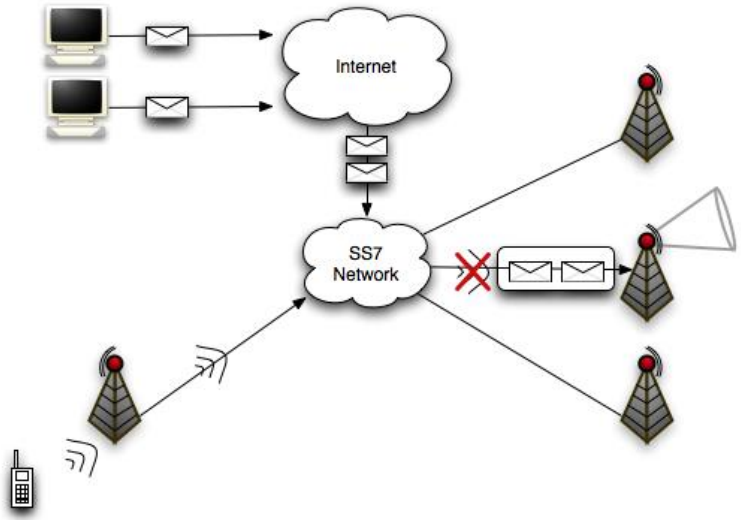

Figure 1. Ubiquity of Internet as an Indispensable ICT Infrastructural Facility.

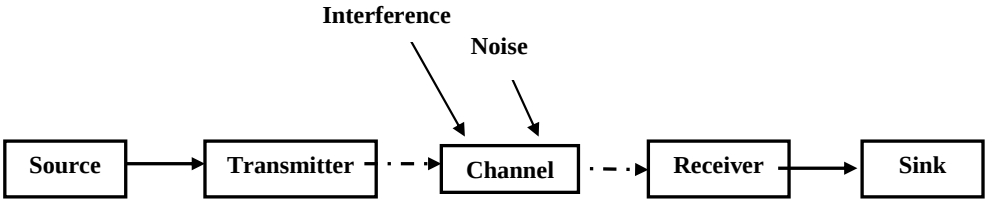

Figure 2. Block Diagram of a Telecommunication System.

In modern context, telecommunications refers to any technology, service, system, or other resource that provides or ensures transmission of electronic data and information. Telecommunication resources may be voice and data networks, wireless services, high speed data communications, telephones, network servers, switches, or any other device, service or system used in electronic communication transmissions. The location/nature of telecommunication systems is equally diverse: ranging from local or building networks to global networks; from single telephone handsets to communication satellites; and whether dedicated to a specific application or shared by many users, programs, and applications. [4]

Generally, the security requirements for telecommunications should not be seen as an isolated phenomenon. Rather, security considerations for telecommunication resources should always take into account the fact that telecommunication is integrally an essential and critical

resource for the functioning of cross-industrial businesses in connection with Information Technology (IT), within the context of the Information Society in our modern global village.

In addition, the applications and transmissions over telecommunication resources must be understood to be essential and critical as well. Just as data or a computer-based network must have appropriate security, so a telecommunication network, which may often be the same network, must have equivalent security. For instance, Password Security requirements for telecommunication resources are the same as those for other IT resources, except for telecommunication devices and resources that have no capability for password protection, such as standard voice termination units (telephones). [4]

In view of the forgoing, this chapter will provide a brief coverage of the subject matter by first assessing the context of security and the threat-scape. This is followed by telecommunication system security requirements; identification of security threats to telecommunication networks, the conceivable counter or mitigating measures and the implementation of those measures. It would also attempt a projection of the telecommunication network security. All these would be preceded by an effort to clarify the telecommunication network security environment, using relevant ITU-T[1*] recommendations and terminologies for secure telecommunications.

2. Conceptual clarifications on Security in Telecommunications and Information Technology

2.1. Basic Security Architecture and Dimensions

As provided by ITU-T guidelines, [5] Recommendation X.805 defines the framework for the architecture and dimensions in achieving end-to-end security of distributed applications. The general principles and definitions apply to all applications, even though details such as threats and vulnerabilities and the measures to counter or prevent them vary, based on the needs of an application.

The security architecture is defined in terms of two major concepts;[6] layers and planes. Security layers address requirements that are applicable to the network elements and systems that constitute the end-to-end network. The three layers are infrastructure layer, services layer and applications layer. One of the advantages of defining the layers is to allow for re-use across different applications in providing end-to-end security. The vulnerabilities at each layer are different and thus counter measures are to be defined to meet the needs of each layer.

The Infrastructure layer consists of the network transmission facilities as well as individual network elements. Examples of components that belong to the Infrastructure layer are individual routers, switches and servers as well as the communication links between them.

The Services layer addresses security of network services that are offered to customers. These services range from basic connectivity offerings, such as leased line services, to value added services like instant messaging.

The applications layer addresses requirements of the network-based applications used by the customers. These applications may be as simple as email or as sophisticated as

[1 *] International Telecommunications Union - Telecommunication Standardization Sector

collaborative visualization where very high-end video transfers are used in oil exploration, or designing automobiles, etc. Further details of ITU-T security guidelines, other related matters are in [6].

3. The Context of Security and the Threat-Scape in Cyber Warfare

The bulk of this segment of the chapter and what follows it to the end of the chapter is taken from an ongoing research work at the School of Engineering, Design and Technology, University of Bradford.[7] It will cover security concepts, security engineering in context, a brief overview of cryptology(cryptography, cryptanalysis), social engineering, Distributed Denial of Service (DDoS) attack, IP Trace-back mechanism and the threat-scape in cyber warfare. This segment will be closed with some deductions.

3.1. Security Concepts

A look up on *security* in dictionaries yields a general view that *security* is "freedom from danger, risk or loss" [8,9]. In the context of this research work, we are concerned with dangers, risks and losses associated with computers, its information/data and network communication transactions. Fundamentally, the need for cryptography arose in response to the requirements to secure information, whether in storage or transit. The most primary security needs it sets out to address are *confidentiality*, *integrity*, *availability* and *authenticity*.[10]

Confidentiality relates to the secrecy or privacy of information; keeping it free from the danger of being exposed to unauthorised parties. Integrity has to do with the need to keep information free from the danger of alteration by unauthorized parties, to prevent it from becoming invalid. Availability is the need to safeguard information against the danger of being lost; ensuring that it is always around and available at the time of need. The fourth critical requirement of information security, authenticity, is the need to make sure that the author or source of our information is the party that claims the responsibility for originating it, and indeed the party we would wish ought to have originated it. The authentication process ensures that an intruder should not be able to camouflage as someone else. It also facilitates *non-repudiation*; that is, a sender should not be able to falsely deny later that he was the originator of a message.[11]

While authentication is used for the symmetric (*private-key*) cryptography, its equivalent in asymmetric *(public-key*) cryptography is the *digital signature*. An authentication is implemented by means of a Message Authentication Code (MAC) generated by the sender, with an authentication key which is shared by the sender and the receiver. On the other hand, certification of each participant's public key is effected via the digital signature of a Certification Authority (CA) in a Public Key Infrastructure (PKI) scheme.[12]

Above concepts are vital security requirements for social interaction using computers or telecommunication systems, just as they are in face-to-face interactions: that someone is who he claims to be; that someone's credentials, whatever type, are valid; and that a document purporting to have come from a person actually came from that person. These are the functions of authentication, integrity, and non-repudiation, respectively.[11]

In assessing security problems in a system, it is important to appreciate several characteristics of the system's security posture. These must include the *threats, vulnerabilities* and *risks.*[10]. Threats are the events, issues or entities that can potentially do harm to the security of the system; these may be intentional or otherwise, including natural disasters. Vulnerabilities are the channels or means that make it possible for or engender a potential ability for harm to afflict the system; they are opportunities for harm to occur. For instance, lack of balanced diets makes a person vulnerable to diseases, or leaving the gate unlocked amounts to a vulnerability in the physical security of the house. Lastly, risks are said to exist where both threats and vulnerabilities co-exist. In other words, a threat to a system that can actually use an already existing vulnerability to compromise the security of the system creates a risk. For example, in an army that is facing a completely illiterate enemy, writing down the orders at all, in plain text, constitutes vulnerability, but there is no risk associated because there is no corresponding threat, since the enemy lacks the ability to read the message. Usually, in a systematic risk analysis to determine the potential problems in the security of a system, it is useful to create a matrix of the various threats and vulnerabilities associated with the system (Risk Assessment Matrix).[10]

3.2. Security Engineering in Context

Security engineering deals with the building of systems that would remain dependable in the face of malice, error and mischance. It concentrates on the tools, processes and methods required to design, implement and test complete systems, as well as to adapt existing systems as their environment changes. These require cross-disciplinary expertise covering cryptography, computer security, hardware temper-resistance, knowledge of economics, applied psychology, organizations and the law [13]. On its own, modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering. Thus, good security engineering requires an amalgamation of four elements.[13] There is need for the policy; the objectives set out for achievement. Then the mechanism; such as the ciphers, access controls, hardware tamper-resistance, and other machinery that would be gathered in order to implement the policy. We also need assurance; the degree of reliance to be placed on each mechanism. Lastly, there is the incentive; the motives which the people protecting and maintaining the system have to enhance optimum performance, as well as the motives that the attackers have in trying to defeat the policy.

All of these elements must interact as illustrated in Figure 3. There is always the tendency to build security around technology, thereby neglecting the most important factor of any security system; *the human factor*. Security revolves around people; both the people who attack the systems, as well as the trusted ones who defend those systems. The people, who must be trusted, in order for the system to function, constitute the most critical element of any security system. This is because they are the most resilient and the only ones endowed with real initiatives. They take decisions, they improvise and they are the most skilled at detecting attacks. However, as components of a security system, human beings are double-edged swords. They suffer from fatigue and can be distracted, tricked and even compromised. Due to their privileged access, when trusted people become compromised they can carry out attacks that outside criminals might find difficult to even contemplate. Therefore, the best

trick is to design security systems that maximize the positive aspects of people, while minimizing their negative aspects.[14]

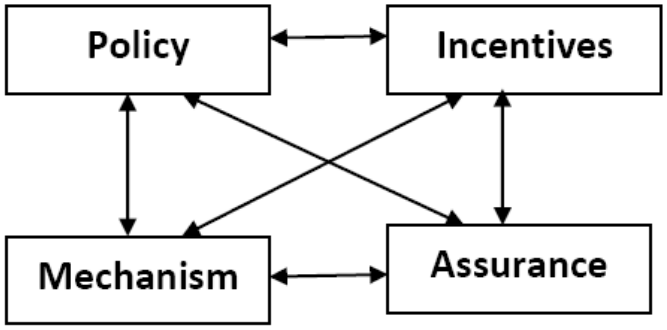

Figure 3. Security Engineering Analysis Framework.

3.3. A Brief Overview of Cryptology

A cipher system or cryptosystem is a technique used to protect messages against unintended recipients. It is made up of an algorithm and all possible plain texts, ciphertexts and keys. A *cryptographic algorithm* is the mathematical function used for encryption and decryption.[15] The decryption algorithm is usually the reverse of its encryption counterpart; for instance, addition and subtraction. *Cryptography* is the art and science that creates cryptosystems while *cryptanalysis* is the art of breaking such systems; that is, reading them even if one is not an intended recipient and does not possess a valid decryption key.

The term *cryptology* is used to encompass both cryptography and cryptanalysis. The original message which is to be sent is called the *plaintext* while the encrypted message is the *ciphertext*. *Encryption* is the process of transforming the plaintext into ciphertext, by using an *algorithm* and a *key*. A key is that component which may be shared secretly or publicly by those that have legal dealings with the message, and may vary from one message to another.

The key is often referred to as a *cryptovariable*. *Decryption* is the process of transforming the ciphertext back to the original plaintext. This reverse process is derived from the knowledge of the encryption algorithm and the key.[15,16]

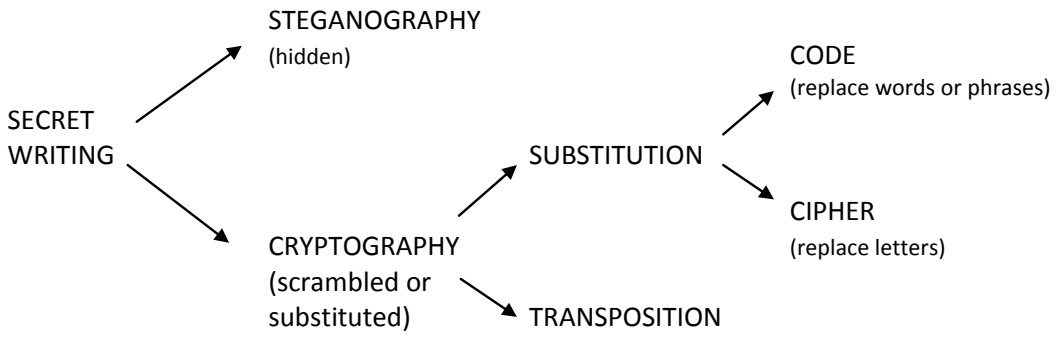

Figure 4. The Science of Secret Writing and its Main Branches.

As provided by Kerckhoff's principle, *a cryptosystem should be secure even if everything about the system, except the key, is public knowledge.* The same idea is expressed in Shannon's maxim as '*the enemy knows the system,*' in contrast to '*security through obscurity'*[17].An illustration of the science of secret writing and its main branches is in Figure 4.[18]

As an illustration, assume the number 786 is to be sent using a cryptosystem, and both parties have agreed on a key value of 019. Using an encryption algorithm, which is the addition of the message (786) and the key (019), the ciphertext is 805. Since the recipient knows the key (019) and the encryption algorithm (addition), the message can be decrypted from the ciphertext by doing the reverse operation, subtracting 019 from 805 to get the plaintext message 786. Anybody intercepting the communication should have some difficulty figuring the plaintext from the ciphertext without the key, even if the encryption technique is known.

3.3.1. Context of Cryptography

Cryptography *is the art and science of keeping messages secure*;[11] *encryption is its original goal.*[12] It is the science of using mathematics to encrypt and decrypt data, thereby making it possible to store sensitive information or transmit it across insecure networks (e.g. Internet), such that it cannot be read by anyone except the intended recipient; using an appropriate decryption key. It is about constructing and analyzing protocols and algorithms that overcome the influence of adversaries, who include eavesdroppers, hackers and cyber warriors. These are related to various aspects in information security, such as data confidentiality, data integrity, and authentication/digital signature; as well as non-repudiation [11,12,19]. Modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering.

Cryptography could be likened to a lock in the physical world. A lock, on its own, is useless until it is part of a larger physical system, such as a door on a building, a chain, a safe, a car, etc. This larger system also includes the people whose roles are crucial in order for the lock to function at all, and to do so effectively. Similarly, cryptography on its own is useless until it forms part of a larger security system; and it is only a very small part of it. As illustrated in Section 3.2, it is only one item under the security mechanism, while the entire mechanism itself is only one out of four major areas of security engineering concerns. However, though it is a small part, cryptography is nonetheless a very important part because, unlike the lock which only denies or grants access to all, cryptography also performs the sensitive function of distinguishing between *good access* and *bad access.* [12]

From the foregoing, it is obvious that the effectiveness of a cryptosystem can only be assessed within the context of the entire security system, of which the *human factor* is the weakest link. Again, it must be noted that the human factor is the most critical factor in the security system for at least three possible reasons; it is the weakest link, the only factor that exercises initiatives, as well as the factor that transcends all the other elements of the entire system. This underscores the significance of *social engineering* in every security arrangement.

3.3.2. General Model of Cryptosystems

Figure 5 illustrates the flow of information in a general cryptosystem. Given the following denotations:

M=P = Plaintext (Message)
E=Encryption Function
D=Decryption Function
K_1=Encryption Key
K_2=Decryption Key
C=Ciphertext (Encrypted Message)

The encryption and decryption operations are respectively governed by the equations:

$$E_{K_1}(M)=E_{K_1}(P) = C \tag{1}$$

$$D_{K_2}(C)=D_{K_2}\{E_{K_1}(M)\} = M = P \tag{2}$$

where K_1 may or may not be the same as K_2; for Symmetric and Asymmetric Cryptography respectively.[98] Where $K_1 = K_2$ for a symmetric operation:

$$E_K(M)=E_K(P)=C \tag{3}$$

$$D_K(C)=D_K\{E_K(M)\} = M = P \tag{4}$$

For symmetric cryptography, the key, which is kept secret, is known only to the sender and receiver. Thus, for '*n'* users, the number of keys required is: [20]

$$^nC_2 = \frac{n(n-1)}{2} \tag{5}$$

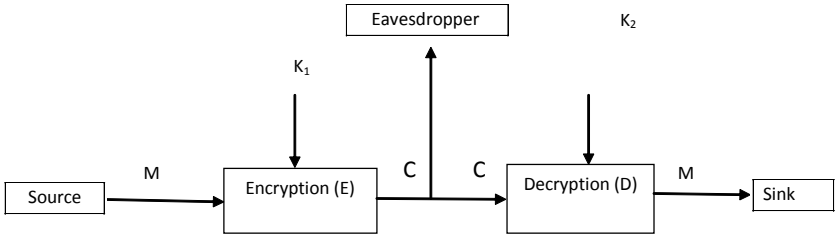

Figure 5. Characterisation of a General Cryptosystem.

For asymmetric cryptography, however, the encryption key K_1 is publicized while the decryption keyK_2 is kept secret by the owner.

3.3.3. Cryptanalysis

It is recalled that the main purpose of cryptography is to keep the plaintext and/or key secret from eavesdroppers (adversaries, attackers, interceptors, interlopers, intruders, opponents, or enemies). Eavesdroppers are assumed to have complete access to the messages in the communication channels, as well as having complete knowledge of the algorithm. The science of recovering an encrypted message without having the decryption key is called *cryptanalysis.* For cryptanalysis to be adjudged as successful, it may recover the plaintext or the key. It may also find sufficient weaknesses that could lead to the breaking of the cryptosystem. If the key is lost through a non-cryptanalytic means, this is termed a *compromise*, while an attempted cryptanalysis is known as an *attack.* There are four general types of cryptanalytic attacks; namely, *ciphertext-only attack, known plaintext attack, chosen-plaintext attack* and *adaptive-chosen-plaintext attack.* Other types of attacks include *chosen-ciphertext attack, chosen-key attack* and *robber-hose cryptanalysis.*[15, 20]

3.4. Social Engineering

In the context of security, Social Engineering (SE) is understood to mean the art of manipulating people into performing actions or divulging confidential information.[21]

SE is a term that describes a non-technical intrusion that relies mainly on human interaction and often involves tricking other people to break normal security procedures.[22]

Defining SE as the art or science of "skillfully maneuvering human beings to take action in some aspect of their lives," [23] Hadnagy noted that SE does not consist of just any one particular action. Comparing it with a delicious meal, which is not just one ingredient, but made up of a careful combination of mixing and adding of many ingredients, SE is a collection of the skills identified in its framework, [24] which, when put together, make up the action and the science.

All social engineering techniques are based on specific attributes of human decision-making, known as cognitive biases. These biases, sometimes called *bugs in the human hardware*, are exploited in various combinations to design attack techniques; such as pretexting, diversion theft, phishing, baiting, tail-gating and phone phishing or Interactive Voice Response (IVR)[25]

In practice, the trade usually involves the use of some form of *confidence trick*; an attempt to defraud a person or group by gaining their confidence. A *confidence artist* is an individual operating alone, or in concert with others, who exploits characteristics of the human psyche; a taxonomy of user vulnerabilities include dishonesty, honesty, vanity, compassion, gullibility, curiosity, courtesy, diffidence, apathy, irresponsibility, naivety and greed.[26,27]

As an act of psychological manipulation, SE had previously been associated with the social sciences.

However, nowadays, its usage has gained popularity among computer professionals.[28] Though 'con game' itself might be as old as humanity, in its present format and nomenclature, a relatively extensive literature search shows that, it is difficult to come by textbooks on SE which were published before 2002; this research effort did not come across any written material before 1995.

Thus, it could be said that, in the security context, the discipline is a recent phenomenon. It seems that this fact emboldened Hadnagy to conclude that his book, *Social Engineering; the Art of Human Hacking,* "covers the world's first framework for social engineering."[17]

3.5. Distributed Denial of Service Attack

A Denial-of-Service (DoS) attack is effected by bombarding the target(e.g. website or transmission medium) with such a volume of requests that it cannot cope with the quantum rise in demand. The website will be slowed down, and, in extreme cases, it will be overwhelmed to the point where it simply stops working.[29] This results in complete service denial for the clients using the website; hence, the term DoS.

The DoS attack is usually carried out by a remotely controlled network of *compromised* or *possessed computers* (bots, zombies; in a botnet) which are *distributed* (scattered) across geographic, political and service provider boundaries; hence, the term DDoS. The end-users whose machines (PCs) are employed are innocent of the attack, as their machines are remotely programmed to attack a target that is designated by the *botnet controller*. These machines are usually broadband-connected. This cyber traffic jam, considered as the most insidious type of attack that exists today,[30,31] is virtually unstoppable because of the ineffective administration of the end-user machines and ubiquity of the botnet coverage. This is further compounded by the fact that bots are programmed to take commands from multiple controller systems. Thus, any successful attempts to destroy a given controller result in the bots simply homing to another controller.

The bot recruitment is implemented by using Trojan horses or viruses, sent to the user in e-mail. The email content automatically forwards itself to all the destinations that are stored in the victim's address book. This attack will continue by the virus propagating itself throughout a system, and subsequently infect one organization after the other. Examples of this kind are the '*I Love You'* and '*Internet Worm'* viruses.[32] The five entities that may constitute a botnet attack are:[30]

- Botnet Operator - This is the individual, group or country that creates the botnet, including its setup and operation. It is the operator that benefits from financial gains, when used for the purpose. Evidence-backed identification of botnet operators has been very difficult for both the law enforcement and cyber security initiatives.
- Botnet Controller - The set of servers that command and control botnet operations. Usually, this is a server that has been maliciously compromised for this purpose, without the knowledge of the real owner. Controller activities include all recruitment, setup, communication and attack. Typical botnets include a handful of controllers distributed across the globe in a non-obvious manner.
- Collection of Bots- These are the end-user broadband-connected PCs infected with botnet malware. They are usually owned and operated by bona fide citizens who are unconsciously used as instruments in a botnet attack. When a botnet includes a concentration of PCs in a given region, observers often incorrectly attribute the attack to that region. It is projected that the use of smart mobile devices in a botnet will grow as upstream capacity and device processing power increase.

- Botnet Software Drop - Most botnets include servers that are designed to store software that might be useful for the botnets during their life-cycle; this is akin to a military arsenal. Like controllers, botnet software drop points are usually servers that have been compromised for this purpose; often unknown to the normal server operator.
- Botnet Target - This is the location that is targeted in an attack. It is usually a website, but, in practice, it can be any device, system or network that is visible to the bots. Mostly, the targets are prominent and controversial websites, simply because they are visible via the Internet and have a great deal at stake in terms of their availability.

In addition to the Russia-Estonian attack of April 2007, the websites of Facebook, Twitter and the blogging pages of Google came under sustained DDoS attacks on 6 August 2009; Goggle managed to survive the attacks, but the other 2 sites were brought down for several hours. It was later understood that the attacks came from Russia, targeting a Georgian blogger called '*Cyxymu'*.[29]

Any serious present study on cyber security must acknowledge the unique threat posed by botnets, because virtually every Internet-connected system is vulnerable.

The arithmetic of the situation is especially intimidating;[30] a botnet that might steal about 500 Kbps of upstream capacity from each bot would only need three bots to collapse a targeted T1 connection.

Thus, only 16,000 bots would be required, theoretically, to fill up a 10-Gbps connection.[30]

The threat is obvious, since most of the thousands of botnets that have been observed on the Internet are at least of this size; many prominent botnets like *Storm* and *Conficker* have several million bots. Thus, the national infrastructure faces a severe threat.

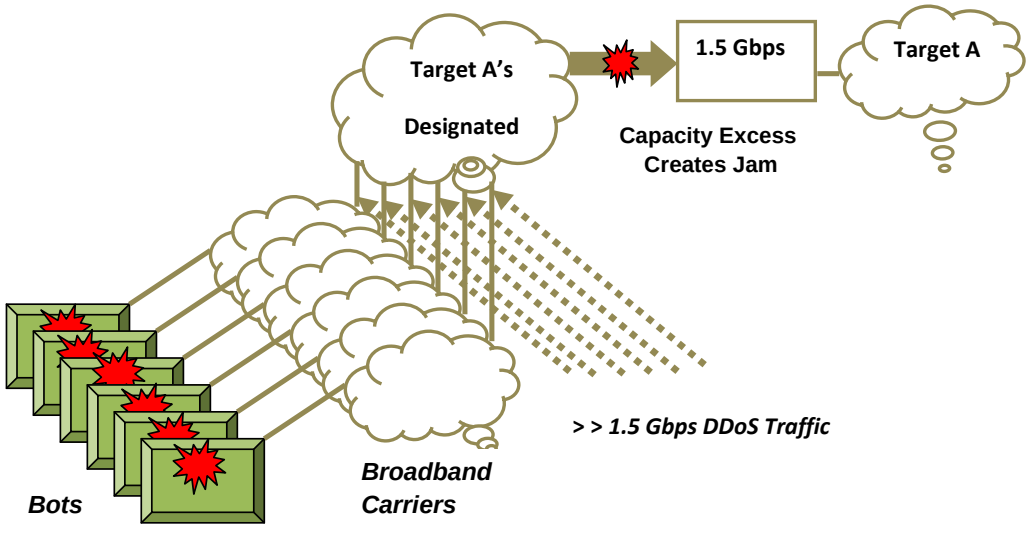

Figure 6. A Sample DDoS Attack from a Botnet.

Illustration

As an example, consider a hypothetical gateway which allows for 1.5 Gbps of inbound traffic, and a botnet creates an inbound stream much larger than 1.5 Gbps. It is obvious that a logjam would result at the inbound gateway, and a DoS condition would occur as illustrated in Figure 6.[30]

3.6. IP Trace-Back Mechanism

The problem of finding the source of a transmission packet is called an IPTrace-back problem. Thus, IP trace-back is a means or method for "reliably determining the origin of a packet on the Internet."[33] The relevance of IPTrace-back technology can only be fully appreciated if the prevalence of the variety of active cyber-attacks on the Internet is reflected upon. Specifically, operators of every Internet Services Provider (ISP) consider the Distributed Denial of Services (DDoS) attacks as the most potent in this regard.[34] The detection and countering of a DDoS attack source is particularly difficult because the IP network is basically stateless with multi-management domains, and the source IP spoofing (camouflaging or faking) is easy. Thus, the IP Trace-back Technology is designed to trace and locate the source(s) of packet transmissions with a focus on countering DDoS attacks [33, 34].

As illustrated in Figure 7, in the IP trace-back mechanism, the user (victim) at a linked terminal unit first issues a tracking request for a packet that is considered to be *an attack*. A piece of packet data is encoded with a unidirectional hash function and transferred to a trace-back system within an Autonomous System (AS) to which the user belongs. The requested trace-back system examines each packet to determine whether it is coming in from an external source or from its own system. When the issued packet is coming from a neighbouring AS, a trace request is queried to the AS. This process is repeated recursively until the trace-back system identifies an actual AS to which the attack source belongs.[34] Although practical tests have demonstrated that tracing the original source of Internet communications is feasible, there are still loose ends to be tied up before the technology becomes a market reality.[34]

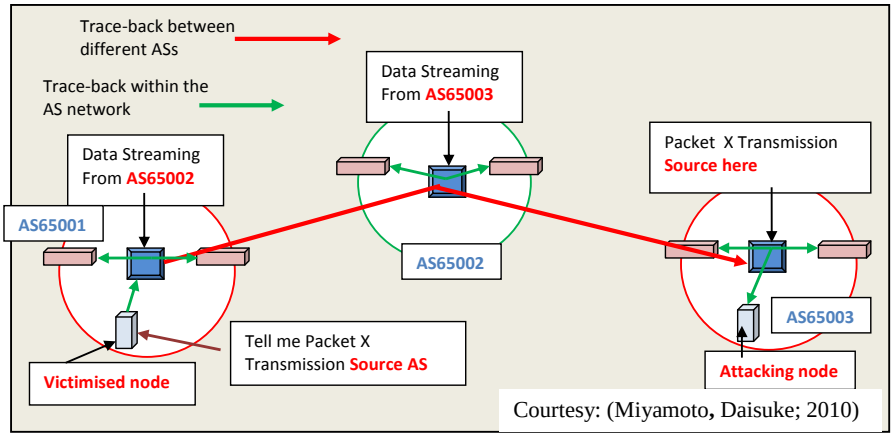

Figure 7. Mechanism of IP Trace-back Technology.

3.7. The Threat-Scape in Cyber Warfare

Whether it was under Sun Tzu, Napoleon Bonaparte, Alexander the Great or our contemporary world, no analysis of war can be made without an understanding of the enemy forces and their composition, disposition, strength, centres of gravity and terrain. [35]. In this virtual warfare, the battle space consists of the cyberspace as defined in Section 3.8.1, while the weapons consist of the various cyber tools, especially the computer/Internet, employed in cybercrimes. These crimes include hacking, botnet, phishing, cyber bullying, cyber stalking, virus attacks, malware/spyware attacks, fraudulent websites, denial-of-service attacks, ID theft(impersonation to commit fraud), cyber terrorism, cyber war, etc.

The threats are classified into the *most active threats* (in terms of actors) and the *most dangerous threats* (in terms of impact)[35]. In descending order, the threat-scape in terms of the amount of cyber activities is dominated by the script kiddy, criminal, hacker groups, insider, political/religious groups and APT/Nation state(Advanced Persistent Threat; military and affiliated groups that may receive support from the government)). Of these, the *malicious insider* is adjudged to be the most dangerous group; they are estimated to represent only about 20% of the threat but cause about 80% of the damage.[35] Researches have shown that, in terms of damages caused, the impact of the activities is almost in reverse order, compared to the prevalence of activities. Thus, in descending order, the threat-scape in terms of the impact of cyber activities is dominated by APT/Nation state, insider, terrorism, physical/environmental attacks (both natural and man-made), criminal/phishing attacks, hacker groups, unintentional actions, hacktivism and Noob/Script kiddy. The *motivations* for cyber-attacks are varied. They are however influenced by the amount of activities in descending order as follows: money, espionage, skills for employment, fame/status, entertainment, hacktivism, terrorism and war.

3.7.1. The Concepts of Cyber and Cyberspace

As a prefix, *'cyber-'* is used in an increasing number of terms to describe new things that are being made possible by the spread of computers. For instance, *cyber-phobia* means an irrational fear of computers.[36] The term originated from *kybernetes*, the Greek word for *steersman* or *governor*.[37] Its contemporary usage dates back to 1948, when it was first used in *cybernetics*, a word coined by Norbert Wiener and his colleagues. [34] 'Cyber' is mostly used as a prefix to describe a person, thing, or idea as part of the computer and information age. Thus, the word *'cyber',* almost a synonym of computer, could be defined as something of, relating to, or involving computers/computer networks.[8] It is in this context that the Internet is described as the *cyber marketplace*.

Closely related to cyber is the concept of *cyberspace*, a metaphor for describing the non-physical terrain (a virtual world) created by computer systems.[38] For instance, online systems create a cyberspace within which people can communicate with one another (via e-mail), do research, or simply window-shop. Like physical space, cyberspace contains objects (files, mail messages, graphics, etc.) and different modes of transportation and delivery. Unlike real space, however, exploring cyberspace does not require any physical movement other than pressing keys on a keyboard or moving a mouse. Defined as "the online world of computer networks and especially the Internet,"[8] the term *cyberspace* was coined by William Gibson. He first used it in his story "Burning Chrome", in 1982 [39, 40], and it

appeared in his science-fiction novel, Neuromancer, in 1984.[41] The US National Military Strategy for Cyberspace Operations defines cyberspaceas "the domain characterized by the use of electronics and the electromagnetic spectrum to store, modify and exchange data via networked systems and associated physical infrastructures."[35]

3.8. Deductions

In our global village, the cyberspace, characterized by the prevalence of computer/Internet, is synonymous to ubiquity. In such a system, dominated by sundry criminals, where the IP trace-back technology to every individual host is not yet a practical reality due to the ease with which IPs can be spoofed, the turbulence in the cyberspace, given the prevailing threat-scape, could only be best imagined.

Putting cryptography and the entire concept of security in proper perspectives, it must be noted that the human factor is the most critical factor in the security system for at least three possible reasons; it is the weakest link, the only factor that exercises initiatives, as well as the factor that transcends all the other elements of the entire system.

This underscores the significance of *social engineering* in every facet of security arrangement. As components of a security system, human beings are double-edged swords. They suffer from fatigue and can be distracted, tricked and even compromised.

Due to their privileged accesses, when trusted people become compromised they can carry out attacks that outside criminals might find difficult to even contemplate. It is thus not surprising to discover that malicious insiders who represent only about 20% of actors in the cyber world are responsible for some 80% of the damages caused. This might spell doom for the prospect of a successful defence against *socio-cryptanalysis* (social hacking), when the trade becomes perfected.

In response, while technical means continue to improve in technical cyber defence, a lot needs to be done in social engineering to checkmate the rising trend of socio-cryptanalysis. The need to step up efforts at improving the security of passwords and pass-phrases, as it affects human attitude, cannot be over-emphasised.

4. Telecommunications System Security Requirements

The basic approach to be adopted in handling this segment is to first of all identify the security threats, followed by the design for their countering or mitigating measures and means by which these measures are implemented.

4.1. Technical Threats to Communication Security

Modern computer security is based on the taxonomy of security threats which includes *confidentiality, integrity, availability and theft.*[30] These are the primary considerations or pillars in modern '*computer communication security'*. In other words, protections are required to deal with sensitive information leaks (confidentiality), worms/viruses affecting the operation of some critical application (integrity), botnets knocking out an important system (availability), or citizens having their identities compromised (*identity* theft).

It is clear, from the foregoing, that the cyber space faces real global threats from cyber criminals. This calls for a proactive cyber defence mechanism to engender a safe cyber environment. Cyber defence consists of measures and techniques developed to safeguard information and information systems stored on computers and associated networks. Potential threats include the destruction of computer hardware/software and the loss, modification, theft, unauthorized use, observation, or disclosure of computer data.[42] An analysis of the threats reveals a combination of technical and nontechnical means of cyber-attacks. Thus, defensive strategies ought to reflect this mixture as well. While procedural measures and social engineering will counter nontechnical attack approaches, cryptography becomes handy as a tool for technical cyber defence.

4.2. Countermeasures against Threats to Communication Security

Cryptography *is the art and science of keeping messages secure;*[11] *encryption is its original goal.*[12] It is the science of using mathematics to encrypt and decrypt data, thereby making it possible to store sensitive information or transmit it across insecure networks (e.g. Internet), such that it cannot be read by anyone except the intended recipient; with appropriate decryption key. It is about constructing and analyzing protocols that overcome the influence of adversaries and which are related to various aspects in information security, such as *data confidentiality*, *data integrity*, and *authentication.*[19] Modern cryptography intersects the disciplines of mathematics, computer science and electrical engineering. There are several ways of classifying cryptographic algorithms. Figure 8 shows 3 categories [43] based on the number of keys that are employed for encryption and decryption. Basically, as illustrated in Figure 8, cryptography is the conversion of information from a readable state (plaintext) to an apparent *nonsense* (ciphertext) with the aid of an *encryption key* at the source. The resultant *ciphertext* is converted back to the original *plaintext* with the aid of a *decryption key* (which may or may not be the same as the encryption key) at the sink.

Depending on the strength of the encryption key, some ciphertexts may be easily broken, such as some *mono-alphabetic substitution cipers*(e.g. the Caesar Cipher). Others may appear unbreakable, at least within the relevant timeframe. For instance, the *Necronomicon* of Al-Hirra, or Book of the Dead (The Voynich Manuscript) has remained unbroken since 730 CE.[44]

Any of the common security concerns of modern communication security, as highlighted in Section 3.1 threatens our mostly cyber-based national infrastructure. These include confidentiality, integrity, availability, authenticity, non-repudiation and identity theft.[30, 45, 10] These are the primary considerations or pillars in modern communication security. They manifest via an ever-growing list of cybercrimes, as highlighted in Section 3.8, the worst of which is the DDoS attack.[34]

In addressing these pillars of security concerns, which may involve both technical and nontechnical measures, the following means would need to be provided: *identification* – who do you say you are; authentication – how do I know you are who you claim to be; *authorisation*– now that you have been verified, what are you allowed to do; *accountability* – who did what, and, perhaps, who pays the bill? Measures aimed at addressing some of these concerns will be discussed in Section 4.3.

4.3. Cryptographic Solutions for the Technical Threats to Communication Security

Obviously, as soon as the first literate human realized that it was necessary to write down a piece of information, either for storage or transmission/transportation, and there would be undesirable consequences should that bit of information be exposed to his antagonists, the challenge of cryptology became manifest.

As people started figuring out ways of encoding information or trying to understand others' encoded messages, the field kept on developing until it reached the current level of complexity; and the development continues.[10] The common technical problems that have been identified in the course of this development relate to the threats of *eavesdropping, modification, replay, masquerading (impersonation, identity theft), penetration* and *repudiation*, as well as their highly sophisticated techniques of accomplishment. From inception, cryptography has been struggling to find solutions to these problems. The cryptographic countermeasures designed to meet these challenges include mechanisms aimed at ensuring *confidentiality, integrity, availability* and *authenticity*, as discussed herein.[32]

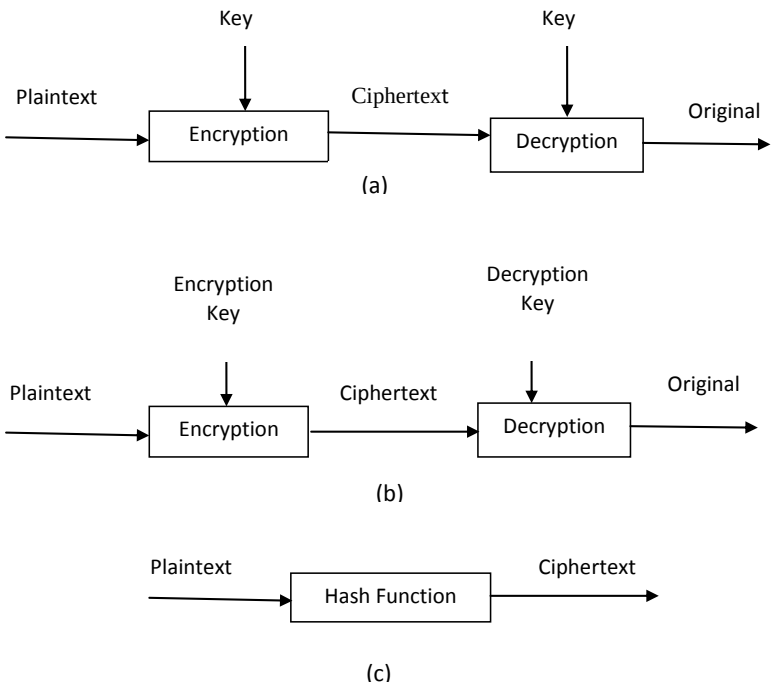

Figure 8. Cryptographic Settings for Secret-key, Public-key, and Hash Function (a, b and c respectively).

4.3.1. Confidentiality

The confidentiality of a message in any form is guaranteed by encryption with a secret key, as long as only the legitimate users have access to that key. Thus, symmetric encryption can provide confidentiality of a message. An eavesdropper would not be able to read the plaintext without the key, even if he acquires the ciphertext. Although asymmetric encryption

could also be used to achieve the same objective, it is strongly argued that, for the purpose of confidentiality, symmetric encryption is favoured over its asymmetric counterpart. This is mainly because of its relative advantage in the speed of execution. However, as the characteristics of both methods are useful in message protection, hybrid systems are often employed to combine their relative advantages.

4.3.2. Integrity

Messages and files require protection against surreptitious modification. While confidentiality procedures offer protection against eavesdroppers, they give little protection against modification and integrity of the message or file. This is critical for text and data messages which are vulnerable to this form of attack. This is particularly instructive in the banking and other financial arenas, where an intruder may be able to change monetary values and account numbers, in a standard transaction form, without the need to actually read it (except for *non-malleable* encryption algorithms). The solution to integrity threat is to employ digital signatures, MACs or some other redundancy scheme in the plaintext prior to encryption. Digital signature is discussed in Section 4.3.5.

4.3.3. Availability

A basic but very fundamental essential in communication security is the control of availability and access to the medium, sensitive data and cryptographic equipment. This involves mainly the issues of physical access control, PINs and passwords. While physical access control is beyond the scope of this discussion, passwords is reserved for some attention in Section 4.3.7.

4.3.4. Authentication

In voice transmission using high-quality transceivers, voice recognition is the obvious authentication method, where the receiver is familiar with the voice of the sender. However, if the two parties are not familiar to each other or the voice quality of the transmission medium is not reliable, other measures would be required to ensure mutual authentication. Using symmetric or asymmetric encryption and suitable key management, the basic problem of message authentication can be resolved. The employment of digital signatures, as discussed in Section 4.3.5, is one approach. However, the problems associated with *replay* or *spoofing,* where a third party taps into the medium, records the transmitted message and retransmits it at a later time or date, remain unresolved. Just imagine the confusion that would arise at Station B, Figure 9, if Station A sends the encrypted message "*ENEMY ATTACKING YOUR LOCATION NOW!"* by 8:00 AM and Station E (aneavesdropper), who could not even understand the message due to lack of key, records it and retransmits it to Station B at 8: PM on the same day; note that Station B would receive this as an authentic message, since it has not been modified. This highlights the need for *time authentication* to be included in the security package, such that replayed messages would not be decode-able.

Time authentication as a method of message authentication is often associated with voice and fax encryption equipment. The protection is achieved by either introducing a time slot of typically 5 minutes after the original encryption, or modifying the key generator process so that the generator at the receiver will not synchronise with the original generator position at

the transmitter. That is, all equipment within the network must have the same ±5 minutes time setting to be able to decode the ciphertext. The use of time slot is however tricky, in the sense that the receiver must have the capacity to check several time slots at the same time, since two stations with very similar times can be in different time slots. Other authentication methods include the use of time stamps and mutual key agreement. Location-based authentication, one of the latest authentication techniques, will be given more attention in Section 5.

4.3.4.1. Text and Data Message Authentication

Most text and data messages are not *real-time* communication, thus they require a different method of authentication called the Message Authentication Code (MAC). This is illustrated in Figure 10. The MAC is similar to a hash function. However, while a virus can be used to modify a hash function, the MAC cannot be modified in the same way, because it relies on a key that is known only to the users.[32] Authentication using encryption with symmetric algorithm has its limitations, but the application of asymmetric encryption using the RSA algorithm guarantees the authenticity of the message. This is because if an encrypted document can be decrypted by a public key, it implies that the message must have been encrypted with the private key pair. This is discussed further in Section 4.3.5. The MAC is encrypted using the secret key and the result is attached to the message that is sent to the receiver. At the receiver the encrypted MAC header is removed from the message and decrypted using the secret key. The resulting calculation is then compared with the original plain MAC value from the message. If the two quantities are the same, this verifies the integrity and authenticity of the message.

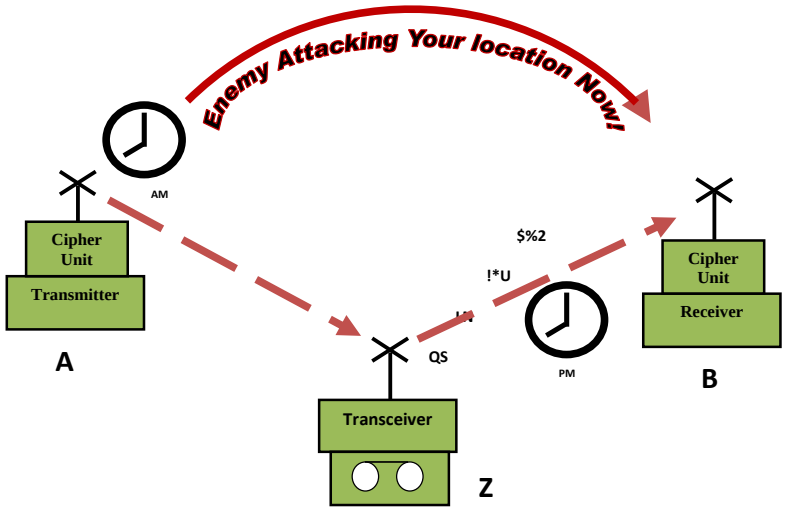

Figure 9. The Need for Time Authentication.

4.3.5. Digital Signatures

Digital signatures are the public key equivalents of MACs. A digital signature is an asymmetric encryption tool that allows the author of the original message to *sign* his document in such a way that the receiver can verify that what he receives is a faithful copy of

the original. The message generation is illustrated in Figure 11. As shown in Figure 12, any modification of the message during transmission will result in the derived signature being different from the original, thus proving loss of integrity. In generating the message using the RSA system, the sender signs his plain message with his private key and transmits it along with the message to the receiver. The receiver uses his authentic copy of the *public key* of the *key pair* to compare the original signature from the sender's document with that of the received message. This is done by running the *verification algorithm*, using the authentic public key, the plain message and the sender's original signature, as inputs.

The primary purpose of the digital signature is just to check for message integrity. It is not used to encrypt the message, thus, it does not offer confidentiality.

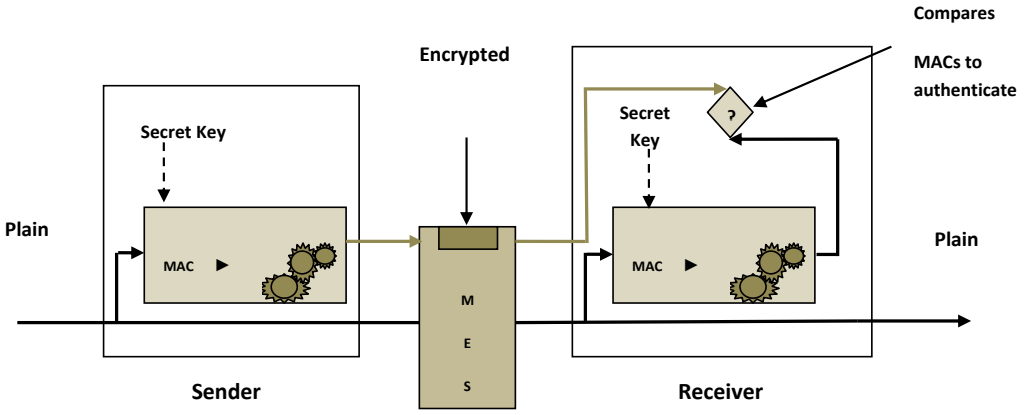

Figure 10. The Message Authentication Code Process (Courtesy: Sutton, R.J., 2002).

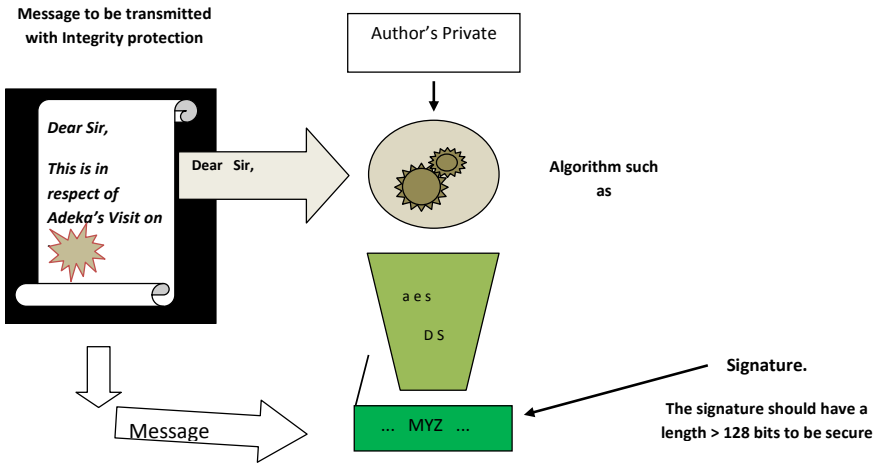

Figure 11. Generation of a Message Signature Using the Author's Private Key. (Courtesy: Sutton, R.J., 2002).

However, by combining the two techniques, where symmetrical encryption of the message text ensures confidentiality, and with signature verification by public key techniques ensuring message integrity, a hybrid system is produced. This results in a very powerful tool that is capable of protecting files and messages. In addition, the use of the public key

encryption to generate and verify the signatures imparts *authenticity* on the message, since only the possessor of the *private key* could have signed the original text, if his *public key* verifies it. Similarly, the originator having signed with his *private key* cannot deny having done this, since he is the only one in possession of his private key. This imparts the feature of *non-repudiation.* In summary, therefore, digital signatures serve the following purposes:

- Public Verifiability - Anybody in possession of the authentic public key can verify the signature.
- Authenticity and Integrity - Modification of a message or its replacement can be detected.
- Non-repudiation - The signatory of a message cannot deny having signed the document.

4.3.6. Key Management

The most secure cryptographic algorithm/protocol is virtually useless without an efficient and effective key management. It is understood that key management is the Achilles heel of most secure communication systems.[32] Available records indicate that the most effective way to attack a secure communication system is to influence the system's personnel and exploit weaknesses in its management.

Table 1. Estimates of time required to break keys by brute force (Courtesy: Sutton, R.J., 2002)

Key Length (bits)	Key Variety	Tests/Sec/ Computer	Number of Computers	Time Used
40	1.1×10^{12}	10^9	10^3	1.1 s
56	7.2×10^{16}	10^9	10^3	20 h
80	1.2×10^{24}	10^9	10^3	38,000 years
128	3.3×10^{38}	10^9	10^3	1.1×10^{19} years
128	3.4×10^{38}	10^9	$7 \times 10^{9*}$	1.5×10^{12} years

*World population.

It is clear from Table 1 that, even for a known algorithm, in order to break a key by *brute force*, an incredible amount of effort, in both time and logistics, is required. Thus, rather than spending a stupendous amount of money on analytical tools to gain information on a 128-bit key, which is statistically impossible within a useful time frame, it is much easier and less expensive to exploit the weaknesses in the human infrastructure; the weakest link in the security system (due to operational deficiencies and compromise reasons).

The purpose of key management is to reduce the risk associated with these threats/vulnerabilities to the barest minimum, and to process secret keys in such a manner that it is transparent to both the user and the network. The issues that relate to key management include key generation, distribution/installation, activation/use, expiration/revocation and destruction, as briefly highlighted herein.

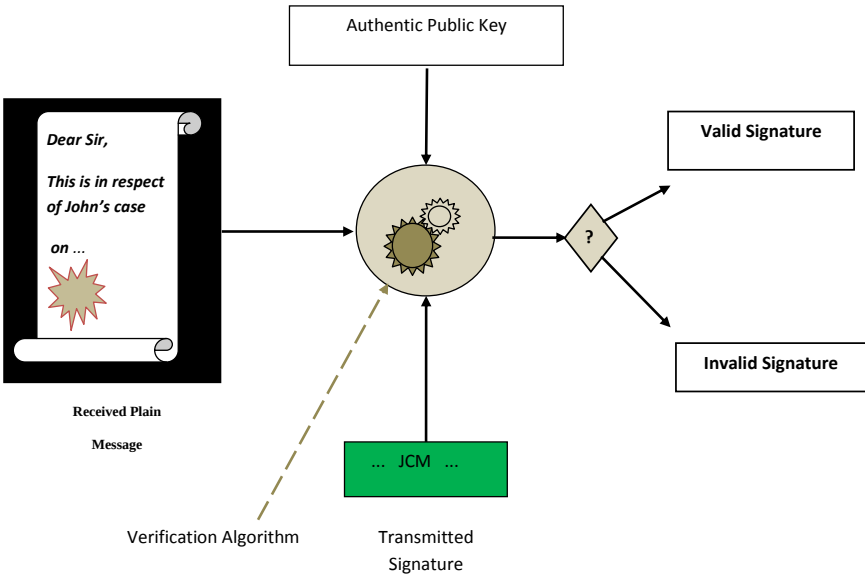

Figure 12. Receiver Runs Verification Algorithm to Detect Modifications to the Message. (Courtesy: Sutton, R.J., 2002).

4.4. PINs, Passwords and Password Security Purgatory

This brief treatment on password security will cover definition, significance, history, categories of access control tools, factors in the security of a password System, multiplicity of passwords with associated problems (storage, length, composition, and attitude), password repositories, security guidelines on password usage, security versus human factors, training/security awareness education and deductions.

4.4.1. Definition and Significance

A summary of definitions indicate that a password or passphrase is a secret word/phrase, string of characters, or some form of interactive message or signal that is used for authentication; to prove identity or gain access to a resource/place.[45,46] Thus, in a nutshell, a password is a basic method of access control. The main function of an access control system is to restrict the use of the resources to authorised users alone. In addition, it limits or defines the degree of access granted to every authorised user.[47] The word *purgatory*, in the context of Section 4.3.7, denotes a miserable situation that is of critical, complex and/or unusual difficulty.[45]

4.4.2. Factors in the Security of a Password System

The security of a system that is protected using passwords depends on several factors. Among these is the need for the overall system to be designed for sound security, with protection against viruses, eavesdroppers and similar threats. Physical security against threats like *shoulder surfing, video camera* and *keyboard sniffers* should also be taken care of.

Passwords should also be chosen such that they are hard to guess and also hard for an attacker to discover using any of the available automatic attack schemes. It is now common practice for the computer to hide passwords as they are being typed as a measure against bystanders reading the passwords. Since this practice may lead to errors and stress, thereby encouraging users to choose weak passwords, experts are now of the view that the system should be designed such that users have the option to show or hide the passwords as they are being typed.[48]

Password strength is a measure of how effective is a password in resisting guessing and brute-force attacks. Usually, this is an estimate of how many trials an attacker who does not have direct access to the password would need, on average, to guess it correctly. The strength of a password is a function of length, complexity and unpredictability.[49]

There are two main factors to consider in determining password strength. These are the number of guesses to find the correct password and the ease with which an attacker can check the validity of each guessed password. The first factor is determined by password length and its measure of randomness; this factor is under users' control. The second factor is determined by how the password is stored and used; this factor is determined by the password system design and beyond control of the user.

Effective access control may force extreme measures on criminals seeking to acquire a password or biometric token.[50] Less extreme measures may include extortion, rubber hose cryptanalysis, and side channel attack.

4.4.3. Security Guidelines on Password Usage

It is usually better to have passwords centrally controlled, if possible. Whatever the case, in order to improve the strength of access security, the following guidelines should be followed in the use of passwords:[32]

- It should be kept absolutely secret; not divulged to any other user
- It should not be written down or recorded where it can be accessed by other users.
- It must be changed if there is the slightest indication or suspicion of a compromise.
- It must be changed when a member of the organization leaves the group or changes task
- It should be at least eight characters long (alpha-numeric with mixed case/symbols)[46]
- It should not be formed from any obvious source; e.g. username or group/company/project name, family name or initials or partner's name, months of the year or days of the week, car number plate registration, nicknames/pet names, telephone numbers, all numeric or all alphabetic characters and more than one consecutive identical characters)
- It must be changed monthly or at least bi-monthly
- It must be changed more frequently the greater the risk or more sensitive the assets being protected
- It must not be included in an automated log in procedure, i.e. not stored in a macro function
- It should not be a dictionary word[46].

4.4.3.1. Guidelines for Strong Passwords

Guidelines for choosing good passwords are designed to make passwords less easily discovered by intelligent guessing. Common guidelines include: [51, 52]

- A minimum password length of 12 to 14 characters if permitted
- Generating passwords randomly where feasible
- Avoiding passwords based on repetition, dictionary words, letter or number sequences, usernames, relative or pet names, romantic links (current or past), or biographical information (e.g., ID numbers, ancestors' names or dates).
- Including numbers, and symbols in passwords if allowed by the system
- If the system recognizes case as significant, using capital and lower-case letters
- Avoiding using the same password for multiple sites or purposes
- Avoid using something that the public or workmates know you strongly like or dislike
- Use acronyms of mnemonic words/phrases
- Providing an alternative to keyboard entry (e.g., spoken passwords, or biometric passwords).
- Requiring more than one authentication system, such as 2-factor authentication (something you have and something you know).
- Write Down Your Passwords

From the above, it is clear that experts are now divergent as regards whether it is better to write down the passwords or not. Some guidelines advise against writing passwords down, while others, noting the large numbers of password protected systems users must access, encourage writing down passwords as long as the written password lists are kept in a safe place, such as a wallet or safe, not attached to a monitor or in an unlocked desk drawer. Schneier [52] noted that:

> "Simply, people can no longer remember passwords good enough to reliably defend against dictionary attacks, and are much more secure if they choose a password too complicated to remember and then write it down. We're all good at securing small pieces of paper. I recommend that people write their passwords down on a small piece of paper, and keep it with their other valuable small pieces of paper: in their wallet."

In addition, some even argue that the concept of password expirations is obsolete,[53] for the following reasons:

- Asking users to change passwords frequently encourages simple and weak passwords.
- If one has a truly strong password, there is little point in changing it. Changing passwords which are already strong introduces risk that the new password may be less strong.

- A compromised password is likely to be used immediately by an attacker to install a backdoor, often via privilege escalation. Once this is accomplished, password changes won't prevent future attacker access.
- Mathematically, it doesn't gain much security at all:
  - Moving from never changing one's password to changing the password on every authenticate attempt (pass or fail attempts) only doubles the number of attempts the attacker must make on average before correctly guessing the password in a brute force attack; one gains much more security just increasing the password length by one character than changing the password on every use.

However, Password expiration serves two purposes:[54]

- If the time to crack a password is estimated to be 100 days, password expiration times fewer than 100 days may help ensure insufficient time for an attacker.
- If a password has been compromised, requiring it to be changed regularly should limit the access time for the attacker.

4.4.4. Password Security versus Human Factors

A synthesis of security guidelines for password usage shows that there is no common standard for passwords; different systems have different requirements. If this situation is analyzed against the backdrop of the fact that an average user has several passwords, all of which are expected to be strong, in conjunction with unavoidable human fallibility, it is obviously impracticable for any human being to combine all the conditions associated with the password system. Thus, since it is the security of the total system (online, offline, physical, procedural and logical) that is important, it is necessary to think of passwords that would take both human and security factors into consideration.[55] Therefore, in order to ensure password security, we must strike a delicate balance between having enough rules to maintain good security and not having too many rules that would compel users to take evasive actions that would, in turn, compromise security.[56]

The above conclusion buttresses the significance of social engineering in security designs, and the fact that security is indeed a function of both technology and social engineering. Unfortunately, most of the literature materials are only concerned with having strong enough rules; only three articles encountered in this research process focused on the pitfalls of having too stringent password regulations.[55, 57, 58].

4.4.5. Training and Security Awareness Education

Every organization should have a security awareness training policy which ensures that organizations are responsible for not only training their own personnel, but also their agents and contractors that have access to their facilities. Initial training will need to include a review of the requirements and tailored training needs to specific security policies, processes and technology of your organization based on the level of security responsibilities for different segments of users.

A security training program should include awareness education covering the organizational security policy, password maintenance, incident reporting, and viruses;

periodic security reminders conducted as updates to the basic security education; user education concerning virus protection, including identification, reporting and prevention measures; user education in importance of monitoring log-in success/failure, and how to report discrepancies, including employee responsibility for ensuring security of information; and user education in password management, including organizational rules to be followed in creating, changing and ensuring confidentiality of passwords.[59] Personnel should also be informed on the need for the various techniques employed in the organization's password security architecture, which are highlighted herein, as an important means of checkmating social hackers (socio-cryptanalysts).

4.4.6. Deductions

As a basic method of access control, passwords constitute the first line of defence in most computer-based information security systems. However, the measure of user's carelessness relative to password security is amazing. Studies have shown that most of the problems associated with the users' care-free attitude have a lot to do with multiplicity of passwords required of every user. Experience shows that an active Internet user has over 60 passwords and PINs for various applications and services; of these, those with the best memories might not be able to memorize up to 25%. Thus, the resultant problems include storage, password length and composition. As a result, in order to relieve the brain of undue stress, password users resort to attitudes that are inimical to password security. The security risk associated with such attitudes is widespread, as a study showed that 50% of users wrote their passwords down.

Experts are now divided as regards whether it is better to write down the passwords or not. Due to the large number of password protected systems that users must access, some experts encourage writing down passwords as long as the written password lists are kept in a safe place, such as a wallet or safe; not attached to a monitor or in an unlocked desk drawer. Similarly, some even argue that the concept of password expirations is obsolete, because mathematically, the practice of changing passwords frequently does not gain much security at all; one gains much more security by just increasing the password length by one character than changing the password on every use.

A synthesis of security guidelines for password usage shows that there is no common standard for passwords; different systems have different requirements. If this situation is analyzed against the backdrop of the fact that an average user has several passwords, all of which are expected to be strong, in conjunction with unavoidable human fallibility, it is obviously impracticable for any human being to observe all the conditions associated with the password system. Thus, since it is the security of the total system that is important, it is necessary to think of passwords that would take both human and security factors into consideration. Hence, in order to ensure password security, we must strike a delicate balance between having enough rules to maintain good security and not having too many rules that would compel users to take evasive actions which would, in turn, compromise security. This conclusion buttresses the significance of social engineering in security designs, and the fact that security is indeed a function of both technology and social engineering.

As part of security training and security awareness education, organizational personnel should also be acquainted with the need for the various techniques employed in the organization's password security architecture, as an important means of checkmating social

hackers (socio-cryptanalysts). From the foregoing, the security of passwords remains a purgatory issue. Thus, the significance of continual security training and awareness education in all organizations cannot be over-stressed.

5. Location Based Authentication

The issue of trust level that could be associated with the active variables in a system is of great significance for security concerns. Since the human factor is the most critical element in security systems,[61] security perimeter could be defined in relation to the human trust level; via mutual positive identification of the correspondents/devices, using various means of authentication.[61,62] Location-based authentication is one of the latest of these techniques.[61, 63] As regards Location-Based Service (LBS) providers, the identity of a customer remains doubtful as long as his location is unknown. This section highlights the importance of location-based authentication techniques with a focus on the role that Global Positioning System (GPS) could play in optimising this authentication approach.

As a result of the ubiquity of wireless communication systems, culminating in the global Internet, modern technology dictates that reliable means for explicit identification be put in place between/among interacting entities. The process of user identification is generally called authentication. To 'authenticate' is to establish the validity of the claim of a user or an entity. In the cyber world, it means positive verification of a user, device, or other entity in a computer system, often as a prerequisite for granting access to resources in a system. Authentication is among the three processes of AAA (Authentication, Authorization and Accounting), [61, 62, 64] as illustrated in Figure 13. When a user requests for access to the restricted area, he is first authenticated, based on which access is granted or denied. Where access is granted, the controller establishes connection between the user and the restricted area; whether access is granted or not, an account which records the information concerning the user's actions is created. [62]

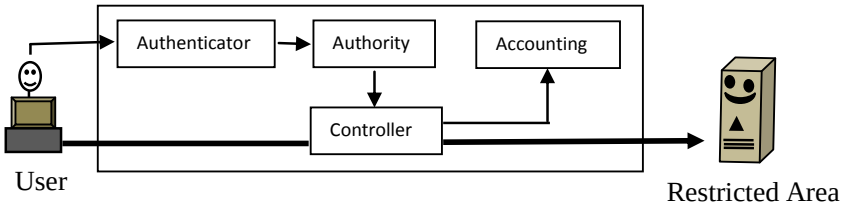

Figure 13. A General AAA System [60].

Authentication techniques are divided into four main categories, based on related authentication factors. These respectively employ the following: [65] *what* you (user) *know* - this is based on knowledge of confidential information (e.g. password); *what* you *have* - techniques using tokens, smart cards, RFID (Radio Frequency Identification Device), hardware keys, etc.; *what* (or who) you *are* – these deal with biometric techniques that are limited to a human authentication, using parameters like the eyes, fingerprints, etc.; and *where* you *are* – this technique is based on the user's physical location; it is a new authentication factor. [63, 65]

The significance of a location-based authentication and some of its applications are discussed in [63, 66, 68]. The usage includes the involvement of physical location as an authentication factor to defeat a cryptographic replay attack by employing the N-Kerberos protocol;[63] in the hospital, a doctor should not handle patients' privacy information beyond the borders of the hospital; an account owner may be denied access to his account unless he is in a secure location, such as the banking environment or at home; senior staff grades may be allowed access to some sensitive data both from home and office, while junior staff grades may be granted access only in a designated location.

LBS encourages new service concepts in tracking applications, with the potential to make many messaging and mobile Internet services more relevant to customers as information is adjusted to context. In this way, location information can considerably improve service usability. Due to the multidimensional benefits of location information, operators now consider it as their *third asset* besides voice and data transmission, with important investment opportunities. These include services related to directions, emergency, transportation of sensitive goods/asset tracking and personal/car navigation; where accuracy is high.[62, 66].

5.1. GPS Capability and Location Based Authentication

The location of a mobile user can be determined in one of two ways; tracking and positioning. If a sensor network determines the location, the mechanism is termed *tracking;* in which case the user must wear a tag or badge to enable the sensor network track his position. The location information is first stored in the sensor network; it is sent to the mobile user on request, via wireless communication. On the contrary, if the mobile system determines the location itself, the mechanism is called *positioning*. In this case, a system of transmitters or beacons sends out radio, infrared, or ultrasound signals. Location information is directly available at the mobile system and does not have to be transferred wirelessly. Similarly, location information is not readable for other users, thus eliminating privacy issues.[66] Tracking and positioning systems are based on the use of basic location techniques, which include: Cell of Origin (COO); Time of Arrival (TOA) and Time Difference of Arrival (TDOA); Angle of Arrival (AOA); Measuring the Signal Strength; Processing Video Data; Triangulation, Trilateration, and Traversing. [62, 66]

Bearing in mind the factors of accuracy, coverage and costs (relative to the user), the satellite positioning technique is the most reliable locating technique; given the current level of technological advancement. This is important because, for a location-based authentication technique to be effective, it ought to be user-centred, otherwise, evasive actions would render it useless. The current capability of theGPS dictates that positioning must be based on own location only; i.e., an entity *'K1'* cannot use his/its GPS receiver data to determine the location of another entity *'K2'* in a different location. That is, using the GPS in location-based authentication necessitates that the user must be the one to supply the own space-time information to the server, and vice versa. Thus, a fraudulent user could supply fake information at will, and vice versa. This has a negative implication on the trust level that authentication is designed to achieve. In order to resolve this problem, it is either a way is found to enable the authenticator use own GPS data to determine the location of the client, or transmission devices are equipped with GPS capabilities to facilitate automatic mutual authentication.[62]

Taking a look at the possible solutions to the problem identified above, it would seem more viable to favour a solution by manufacturers.[62] That is, there would be urgent need to make all transmission devices GPS-compliant, with inherent capabilities for location-based mutual authentication. This recommendation is in congruence with [63], using the N-Kerberos Cryptographic Protocol, which posited that the *P(Y)* code signature should be injected into the user's device to avoid carrying the *GPS* receiver every time. However, privacy issues might arise to oppose this recommendation. This would be a weak argument in the view of [62], given the fact that such devices could be enhanced with enabling/disabling capabilities at the user's discretion; similar to the *Bluetooth* technology.

6. Future Projections

Schneier [69] blamed the worsening network security situation on complexity and what is referred to as *externality* in economics, or *vicarious liability* in law. That is, the security of a network is inversely proportional to its complexity, while externality and vicarious liability refer to the cost of a decision that is borne by people other than those making the decision. He postulated that network security would continue to get worse unless there was a drastic change in the prevailing practice of vicarious liability in the computer/security industry; where consumers of security products, as opposed to producers, bear the cost of security ineffectiveness. Schneier concluded that Security solutions have a technological component but security is fundamentally a people problem.[69] This is because a security system is only as strong as its weakest link, while the weakest link of any security system is the human infrastructure. In this regard, the significance of social engineering as a tool for cyber defence has been underplayed, compared to technological tools like cryptography. Unless this trend is reversed, it is likely that the current state of insecurity in the communication industry will get more compounded as network systems become more complex.

Since the human factor is the most critical element in security systems,[60] security perimeter could be defined in relation to the human trust level; via mutual positive identification of the correspondents/devices, using various means of authentication.[61, 62] Thus, the human security perimeter could be extended using positive authentication. Location-based authentication is one of the latest authentication techniques.[61,63] Bearing in mind the factors of accuracy, coverage and costs (relative to the user), the satellite positioning technique is the most reliable locating technique; given the current level of technological advancement. Hence, it is suggested that all transmission devices be made GPS-compliant, with inherent capabilities for location-based mutual authentication. This could enhance the future of telecommunication security.

Conclusion

Our global age is practically defined by the ubiquity of the Internet; the worldwide interconnection of cyber networks that facilitates accessibility to virtually all ICT and other elements of critical infrastructural facilities, with a click of a button. This is regardless of the user's location and state of equilibrium; whether static or mobile. However, such interconnectivity is not without security consequences.

A *telecommunication* system is indeed a *communication* system with the distinguishing keyword, the Greek *tele-*, which means "atadistance", to imply that the source and sink of the system are at some distance apart. Its purpose is to transfer information from some source to a distant user; the keyconcepts being *information, transmission* and *distance.* These would require a means, each, to send, convey and receive the information with safety and some degree of fidelity that is acceptable to both the source and the sink.

Chapter K begins with an effort to conceptualize the telecommunication network security environment, using relevant ITU-T[2*] recommendations and terminologies for secure telecommunications.

The chapter is primarily concerned with the ***security*** aspect of computer-mediated telecommunications. Telecommunications should not be seen as an isolated phenomenon; it is a critical resource for the functioning of cross-industrial businesses in connection with IT. Hence, just as information, data or a computer/local computer-based network must have appropriate level of security, so also a telecommunication network must have equivalent security measures; these may often be the same as or similar to those for other ICT resources, e.g., password management.

In view of the forgoing, the chapter provides a brief coverage of the subject matter by first assessing the context of security and the threat-scape. This is followed by an assessment of telecommunication network security requirements; identification of threats to the systems, the conceivable counter or mitigating measures and their implementation techniques. These bring into focus various cryptographic/crypt analytical concepts, vis a vis social engineering/socio-crypt analytical techniques and password management.

The chapter noted that the human factor is the most critical factor in the security system for at least three possible reasons; it is the weakest link, the only factor that exercises initiatives, as well as the factor that transcends all the other elements of the entire system. This underscores the significance of social engineering in every facet of security arrangement. It is also noted that password security could be enhanced, if a balance is struck between having enough rules to maintain good security and not having too many rules that would compel users to take evasive actions which would, in turn, compromise security. The chapter is of the view that network security is inversely proportional to its complexity. In addition to the traditional authentication techniques, the chapter gives a reasonable attention to location-based authentication. The chapter concludes that security solutions have a technological component, but security is fundamentally a people problem. This is because a security system is only as strong as its weakest link, while the weakest link of any security system is the human infrastructure.

A projection for the future of telecommunication network security postulates that, network security would continue to get worse unless there is a change in the prevailing practice of externality or vicarious liability in the computer/security industry; where consumers of security products, as opposed to producers, bear the cost of security ineffectiveness. It is suggested that all transmission devices be made GPS-compliant, with inherent capabilities for location-based mutual authentication. This could enhance the future of telecommunication security.

[2*] International Telecommunications Union - Telecommunication Standardization Sector

Acknowledgments

The role of the Petroleum Technology Development Fund (PTDF, Nigeria) for sponsoring the main PhD Programme, which produced this chapter, is hereby acknowledged. The same is true of the Nigerian Army which approved the programme. The authors also wish to appreciate the contributions of the various staffs, departments and students of the School of Engineering and Informatics, University of Bradford, United Kingdom.

References

[1] Network Security Research Centre, (2010). *Telecommunications Security*. [Online]. Available: http://siis.cse.psu.edu/tele.html. [Accessed: 19 November 2012].

[2] P. Traynor, P. McDaniel and T. La Porta, *Security for Telecommunications Networks*, Springer, 2008.

[3] M.I. Adeka, "Optical Fiber Telecommunication Systems: Problems and Prospects," MSc thesis, Department of Electrical Engineering, College of Engineering, Rochester Institute of Technology, Rochester, 1993.

[4] Department of Homeland Security Management Directive System MD Number: 4800.

[5] Security in Telecommunications and Information Technology: An overview of issues and the deployment of existing ITU-T Recommendations for secure telecommunications'. [Online]. Available at: http://www.itu.int/itudoc/itu-t/85097.pdf Accessed: 14 November 2012.

[6] ITU-T Recommendations X.805, 2003 in 'Security in Telecommunications and Information Technology: An overview of issues and the deployment of existing ITU-T Recommendations for secure telecommunications'. [Online]. Available at: http://www.itu.int/itudoc/itu-t/85097.pdf Accessed: 14 November 2012.

[7] M.I.U. Adeka, J.S. Shepherd, and R.A. Abd-Alhameed, "Cryptography and Computer Communication Security: *Social and Technological Aspects of Cyber Defence,"* Ongoing PhD Research Work, School of Engineering, Design and Technology, University of Bradford, Bradford (UK), (Ongoing: 2011-).

[8] http://www.merriam-webster.com/dictionary/cyber?show=0&t=1335771267.

[9] Dictionary.com. *Definitions from Dictionary.com;* http://www.dictionary.com. Based on the Random House Unabridged Dictionary, 2006.

[10] C. Swenson, *Modern Cryptanalysis: Techniques for Advanced Code Breaking.* Indianapolis: Wiley Publishing, Inc., 2008.

[11] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C.* Indianapolis (US): John Wiley & Sons, Inc., 1996.

[12] F. Niels et al., *Cryptography Engineering: Design, Principles, and Practical Applications.* Indianapolis (US): Wiley Publishing, Inc., 2010.

[13] G.K. Warren and G.H. Jay, *Computer Forensics: Incident Response Essentials*. Addison-Wesley, 2002, p. 392.

[14] Schneier, Bruce. *Beyond Fear: Thinking Sensibly about Security in an Uncertain World.* New York: Copernicus Books, Inc., 2003.

[15] D. Kahn, *The Codebreakers: History of Secret Communication.* New York: MacMillan Publishing Co., 1967.

[16] *"An Overview of the History of Cryptology."* [Online]. Available: http://publications.gc.ca/collections/collection_2007/nd-dn/D96-1-2004E.p: [Accessed 1 Oct. 2011].
[17] D. Kahn, *The Codebreakers: A Comprehensive History of Secret Communication from Ancient Times to the Internet,* Revised and Updated. New York: Scribner, New York. 1996.
[18] S. Singh, *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*. New York: Anchor Books, Inc., 1999.
[19] A.J. Menezes et al., *Handbook of Applied Cryptography*. CRC Press. 1997.
[20] M.Y. Rhee, *Cryptography and Secure Communications.* Singapore: McGraw-Hill Book Co., 1994.
[21] J. Goodchild, (11 January 2010) "Social Engineering: The Basics". csoonline. Available: http://en.wikipedia.org/wiki/Social_engineering(security). [Accessed: 15 Jan. 2012].
[22] http://searchsecurity.techtarget.com/definition/social-engineering. [Accessed: 15 Jan. 2012].
[23] C. Hadnagy, *Social Engineering; The Art of Human Hacking*. Indianapolis. Wiley Publishing, Inc. 2011, p.10.
[24] http://www.social-engineer.org/framework/Social_Engineering_ Framework. [Accessed: 15 Jan. 2012].
[25] K. Jaco, "*CSEPS Course Workbook*." unit 3, Jaco Security Publishing, 2004.
[26] J. Long, *No Tech Hacking – A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing*. Syngress Publishing Inc., 2008.
[27] D. Harley, "Re-Floating the Titanic: Dealing with Social Engineering Attacks." *EICAR Conference*, 1998. [Online]. Available: http://cluestick.info/hoax/harley_eicar98.htm. {Accessed: 06 Oct. 2012].
[28] R.J. Anderson, Security engineering: a guide to building dependable distributed systems (2nd ed.). Indianapolis, IN: Wiley, 2008, p. 1040.
[29] S. Ridley and J. Bird, C*ybercrime*. London: Franklin Watts. 2010.
[30] E.G. Amoroso, *Cyber Attacks: Protecting National Infrastructure.* Burlington (US): Elsevier Inc., 2011.
[31] D. Miyamoto**,** "Development of Practical IP Trace-back Technology." *NICT News*, No. 396, September, 2010. [Online]. Available: http://www.nict.go.jp/publication/NICT-News/1009/NICT_NEWS_1009_E.pdf. [Accessed: 07 Oct. 2011].
[32] R.J. Sutton, *Secure Communications: Applications and Management.* Chichester: John Wiley & Sons, Ltd. 2002.
[33] C. Jiayong, "IP Traceback Technology and its Standardization." *ZTE Corporation*, 15 April 2007. [Online]. Available: http://www.itu.int/dms_pub/itu-t/oth/15/04/T15040000100001PDFE.pdf. [Accessed 28 Jan. 2012].
[34] D. Miyamoto**,** "Development of Practical IP Trace-back Technology." *NICT News*, No. 396, September, 2010. [Online]. Available: http://www.nict.go.jp/publication/NICT-News/1009/NICT_NEWS_1009_E.pdf. [Accessed: 07 Oct. 2011].
[35] J. Andress and S. Winterfeld, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners.* Waltham.
[36] http://www.webopedia.com/TERM/C/cyber.html. [Accessed: 07 Oct. 2011].
[37] http://askville.amazon.com/word-cyber-older-modern-eaning/ AnswerViewer.do?requestId=4086267. [Accessed: 07 Oct. 2011].

[38] http://www.webopedia.com/TERM/C/cyberspace.html.
[39] T. Bradley, et al., *Essential Computer Security: Everyone's Guide to Email, Internet, and Wireless Security.* Rockland, MA (US): Syngress Publishing, Inc. 2006.
[40] http://project.cyberpunk.ru/idb/williamgibson.htm. [Accessed: 07 Oct. 2011].
[41] http://www.hatii.arts.gla.ac.uk/MultimediaStudentProjects/00-01/0003637k/project/html/condef.htm .
[42] D.B. Parker, "Computer Security," in *Microsoft ® Encarta.* Redmond, WA: Microsoft Corporation, 2009.
[43] http://www.garykessler.net/library/crypto.html. [Accessed: 27 Sep. 2011].
[44] S.J. Shepherd, *Cryptography: Diffusing the Confusion.* Philadelphia: Research Studies Press Ltd. 2001.
[45] R. Lehtinen et al., *Computer Security Basics,* 2nd ed. Sebastopol, CA (US): O'Reilly Media, Inc.,2006.
[46] M. Bando, *101st Airborne: The Screaming Eagles in World War II.* Mbi Publishing Company, 2007. [Online]. Available at: http://books.google.com/books?id =cBSBtgAACAAJ. [Accessed: 20 May 2012].
[47] D.S. Jeslet et al. "Survey on Awareness and Security Issues in Password Management Strategies*." IJCSNS*, vol. 10, no.4. April, 2010.
[48] Lyquix Blog: Do We Need to Hide Passwords?. Lyquix.com. [Accessed: 17 Sept. 2012].
[49] "Cyber Security Tip ST04-002". Choosing and Protecting Passwords. US CERT. [Online]. Available: http://www.us-cert.gov/cas/tips/ST04-002.html. [Accessed: 20 Jun. 2009].
[50] J. Kent, "Malaysia car thieves steal finger." *BBC News*. 31 Mar 2005. [Online]. Available: http://news.bbc.co.uk/1/hi/world/asia-pacific/4396831.stm. [Accessed: 16 Oct. 2012].
[51] Microsoft Corporation, "Strong passwords: How to create and use them." [Online]. Available: (http://www.microsoft.com/security/online-privacy/passwords-create.aspx). [Accessed: 11 Nov 2012].
[52] B. Schneier, 2005 "Schneier on Security: Write Down Your Password." [Online]. Available at: (http://www.schneier.com/blog/archives/2005/06/write_down_your.html). [Accessed: 25 Sep. 2012].
[53] E. Spafford, "Security Myths and Passwords." *The Center for Education and Research in Information Assurance and Security*. 2008. [Online]. Available: http://slashdot.org/story/06/04/25/0033238/spafford-on-security-myths-and-passwords [Accessed: 21 Sep. 2012].
[54] LOPSA, "In Defence of Password Expiration". *League of Professional Systems Administrators*, April 27, 2006. [Online]. Available at: https://lopsa.org/node/295. [Accessed: 27 Sep. 2012].
[55] E.F. Gehringer, (2002) "Choosing Passwords: Security and Human Factors." *IEEE*, 0-7803-7824-0/02/$10.00 8.
[56] M. Adeka, S. Shepherd and R. Abd-Alhameed, "Resolving the password security purgatory in the contexts of technology, security and human factors," *Computer Applications Technology (ICCAT), 2013 International Conference on* , vol., no., pp.1,7, 20-22 Jan. 2013 doi: 10.1109/ICCAT.2013.6522044

[57] Adams and M.A. Sasse, "Users are not the enemy." *Communications of the ACM 42:*12 December, 1999.

[58] W. Rash, (2002) "Password chaos threatens e-commerce." *Znet Tech Update.* 19 February, 2002. [Online]. Available at: http://techupdate.znet.com/techupdate/ stories/main/0,14179,28,47895,00html. [Accessed: 12 Oct. 2012].

[59] http://www.nesnip.org/securitychapter1.htm#Section%20I [Accessed: 10 Oct. 2012].

[60] G. Lenzini et al., "Trust-enhanced Security in Location-based Adaptive Authentication," Electronic Notes in Theoretical Computer Science, vol. 197, pp. 105-119, 2008.

[61] D. Jaros and R. Kuchta, **"**New Location-based Authentication Techniques in the Access Management," in ICWMC.2010.62, 2010 IEEE. DOI:10.1109/ ICWMC.2010.62.

[62] M. Adeka, S. Shepherd, and R. Abd-Alhameed, "Extending the security perimeter through a web of trust: The impact of GPS technology on location-based authentication techniques," *in Proceedings of the Fifth International Conference on Internet Technologies and Applications (ITA 13),* pp. 465-473, 2013.

[63] N.T. Abdelmajid et al., "Location-based Kerberos Authentication Protocol," in SocialCom.2010.163, 2010 *IEEE*. DOI: 10.1109/ SocialCom.2010.163.

[64] H. Rui et al., "A novel service-oriented AAA architecture," in *Personal, Indoor and Mobile Radio Communications,* 2003. 14th IEEE Proceedings on, 2003, vol.3, pp. 2833-2837.

[65] G. Lenzini et al., "Trust-enhanced Security in Location-based Adaptive Authentication," Electronic Notes in Theoretical Computer Science, vol. 197, pp. 105-119, 2008.

[66] J. Schiller and A. Voisard, "Location-Based Services," in *Location-Based Services*, Jim Gray, Ed. New York: Elsevier Inc., 2004.

[67] Ray and M. Kumar, "Towards a location-based mandatory access control model," *Computers & Security*, vol. 25, pp. 36-44, Feb 2006.

[68] D. E. Denning and P. F. MacDoran, "Location-based authentication: Grounding cyberspace for better security," *Computer Fraud & Security*, vol. 1996, pp. 12-16, 1996.

[69] B. Schneier, *Secrets & Lies: Digital Security in a Networked World.* Indianapolis: Wiley Publishing, Inc., 2000/2004, p.1.